ČESKÁ SPOŘITELNA

POKYNY PRO PŘIJÍMÁNÍ PLATEBNÍCH KARET
při placení zboží a služeb
Transakce typu e-commerce

Obchodní místo je oprávněno přijímat karty:

☒ANO ☐NE VISA[1]

☒ANO ☐NE VISA Electron[1]

☒ANO ☐NE MasterCard [2]

☒ANO ☐NE Maestro[2]

1. Internetová stránka obchodního partnera musí obsahovat:

1. Název obchodního partnera, který je identický s názvem uvedeným na propagačních materiálech a dodacím listě.
2. Loga karet asociací Visa a MasterCard přijímaných k platbě na internetu umístěné na úvodní stránce týkající se prodeje zboží/služby.
3. Bezpečnostní podmínky přenosu dat o platebních kartách, které zajišťuje systém 3-D Secure, včetně log VERIFIED by VISA a MasterCard SecureCode, umístěných na úvodní stránce týkající se prodeje zboží/služby.
4. Nabídku zboží/služeb odpovídající charakteru a předmětu obchodní činnosti.
5. Podmínky pro zasílání zboží/služeb (včetně omezení nebo zákazů, pokud existují).
6. Pravidla pro řešení reklamací/refundací transakcí. Držitel karty musí být před transakcí upozorněn na skutečnosti např.:
   - Obchodní partner nepřipouští výměnu nebo vrácení zboží, nerefunduje transakce.
   - Výměna je možná pouze za stejné zboží nebo ve výši částky původní transakce.
   - Dodací lhůta - v případě, že lhůta dodání zboží je delší než 30 dnů, je nutný souhlas Držitele karty se zasláním v pozdějším termínu.
   - Obchodní partner musí uvádět všechny poplatky a daně na základě obchodního zákoníku (balné a poštovné; pojištění zboží/služeb; daně; DPH; dodatečné poplatky schválené držitelem karty, např. za dodatečné zaslání zboží; specifikaci které z těchto poplatků (DPH) jsou již obsaženy v ceně).
7. Povolenou měnu transakce, která je uvedena symbolem a slovy.

1.1. Oddělení služeb zákazníkům:

1. Všechny platební podmínky a omezení pro transakce musí být zřetelně viditelné před nebo v době transakce (omezení prodeje z důvodu věku, místní omezení, právní omezení). Musí být uvedeny v Potvrzení o transakci.
   Varianty pro umístění těchto informací jsou:
   - Samostatný formulář, kde Zákazník potvrdí, že četl a souhlasí s uvedenými podmínkami před potvrzením transakce.
   - Součástí platebních stránek po provedení nákupu a před ukončením objednávky.
2. Oznámit Zákazníkovi, že vybrané zboží není na skladě a kdy bude opět k dispozici.
3. V případě, že není veškeré objednané zboží k dispozici, nabídnout Zákazníkovi možnosti:
   - odebrání pouze skladového zboží, s pozdější dodávkou chybějícího objednaného zboží,
   - odebrání pouze skladového zboží,
   - odložení celkové dodávky do kompletního plnění objednávky.

1.2. Zabezpečení internetových stránek:

Systémy obsahující citlivá data o Zákaznících musí být co možná nejlépe zabezpečeny. Obchodní partner zodpovídá za bezpečné uložení citlivých dat a průkaznou evidenci k jejich přístupu. Využívá-li obchodní partner služeb třetích stran ke zpracování a uložení těchto citlivých dat, je za tyto třetí strany zodpovědný. Obchodní partner písemně předloží ČS při podpisu Smlouvy bezpečnostní koncept ochrany dat, ve kterém se mimo jiné zavazuje, že zajistí:

- Vymazání a fyzické odstranění všech citlivých údajů o Zákaznících, po stanovené době 5 let, kdy již nejsou potřebné.
- Zabezpečení veškerých přístupů k citlivým datům zadáním uživatelského jména a hesla včetně nadefinování rolí a odpovědností v rámci společnosti, které jsou následně logovány a průběžně kontrolovány. V případě jejich nepoužívání nebo odchodu zaměstnance ze společnosti jsou následně deaktivovány.
- Šifrování jako Secure Socket Layer (SSL) k ochraně dat při vstupu Zákazníků, zaměstnanců nebo obchodních partnerů do systému. Zašifrování citlivých dat o zákaznících v databázích a na zálohovacích médií.

---

[1] Zároveň platí pro Visa Electron debet, Visa Business debet, Visa V-Pay debet, Visa debet ostatní, Visa Electron kredit, Visa Business kredit, Visa V-Pay kredit, Visa kredit ostatní

[2] Zároveň platí pro Cirrus, Debit MasterCard, MasterCard Credit, Maestro, Private label

- Vytvoření krizového plánu pro řešení bezpečnostních rizik, jeho dokumentaci a předání kompetentním osobám k řešení, včetně pravidelného testování bezpečnosti systému a testu vniknutí do systému.
- Implementaci vstupních kontrol na straně serveru tak, aby nebylo možné obejít vstupní kontroly na straně klienta.
- Zabezpečenou konfiguraci routeru včetně instalace vstupních a výstupních filtrů na všech hraničních routerech.
- Instalaci antivirového softwaru na všech serverech a pracovních stanicích a jeho pravidelná aktualizace. Změnu defaultního nastavení bezpečnosti na produkčních systémech dodavatele před zavedením do produkce a následná aktualizace produkčních systémů pomocí nejnovějších bezpečnostních patchů vydaných dodavateli.
- Oddělení segmentu sítě obsahující servery pro umístění webu od segmentu sítě obsahující interní servery firewallem včetně aktualizace a patchování firewallu.
- Aplikace bude resistentní vůči útokům typu Cross-Site Scripting (XSS), SQL Injection, Cookie Stealing, atd. To znamená, že v aplikaci obchodního partnera bude zajištěna řádná kontrola všech vstupních polí.

Součástí bezpečnostního konceptu ochrany dat je obchodním partnerem vyplněný formulář Sebehodnocení bezpečnosti systému obchodního partnera.

1.3. ČS je oprávněna:

1. Prověřit platnost internetových adres (URL).
2. Prověřit propojení s internetovými stránkami obchodního partnera.
3. Stanovit zvláštní pravidla pro kategorii rizikových obchodních partnerů, cestovní služby, předplatné, SW, které je obchodní partner povinen akceptovat.
4. Provádět průběžné kontroly, které je obchodní partner povinen strpět.
5. Požadovat zabezpečení dat Držitelů karet vstupujících na internetové stránky obchodního partnera v jí stanovené lhůtě.
6. Provést kontrolu resistence aplikace vůči útokům typu Cross-Site Scripting (XSS), SQL Injection, Cookie Stealing, atd.

---

2. Transakce

Transakce musí být obchodním partnerem provedena do 7kalendářních dnů od data autorizace.

Obchodní partner nesmí zaslat bez předchozího kontaktování ČS k zúčtování transakce, které by mohly být podvodné a které vykazují jeden nebo více následujících znaků:

- částka Transakce převyšuje průměrnou anebo obvyklou částku transakce na Obchodním místě,
- jedná-li se o opakované zaslání zboží na stejnou adresu během jednoho týdne,
- jedná-li se o opakované objednávky zboží ze stejné e-mailové adresy, během jednoho týdne,
- z jedné e-mailové/IP adresy přijde v jeden den víc pokusů o uskutečnění Transakce,
- z jedné IP/e-mailové adresy je jedna anebo víc Transakcí zamítnutých a další může být schválená,
- transakce přišly z už identifikovaného podezřelého e-mailu/IP,
- objednávka byla zaslána z neobvyklé e-mailové adresy (ne jméno, ale náhodný řetězec znaků a čísel),
- dodací adresa je na neobvyklé místo dodání zboží. Za rizikové oblasti je považována Afrika (Nigérie), Asie (Thajsko), Jižní Amerika (Venezuela) atd. (může se měnit),
- držitel karty žádá urychlené dodání zboží v porovnání se standartní dobou dodání, dotazuje se na přesnou dobu dodání zboží, mění adresu dodání, žádá předání na parkovišti, v hotelu, řidiči taxislužby apod.

V případě jakýchkoliv pochybností o korektnosti Transakce obchodní partner kontaktuje ČS a požádá ji o součinnost při řešení, zda Transakci zrealizovat či nikoli.

2.1. Tři základní režimy nákupu v internetovém obchodě, které jsou podporovány ze strany ČS:

- nákup s okamžitým poskytnutím zboží či služby a bezprostředním zaplacením,
- nákup s pozdější distribucí zboží,
- opakovaný prodej (viz Podporované transakce v bodě 2.2.) - dlouhodobě poskytovaného zboží či služeb s pravidelnou periodickou úhradou.

2.2. Podporované transakce:

1. **Sale/Prodej** - Transakce sloužící pro autorizaci a následné zpracování platební transakce. Je shodná s transakcí prodej na fyzických platebních terminálech. Bude využita pro úhradu zboží a služeb tam, kde bude platba požadována bez odkladu po objednávce.
2. **Pre-autorization/Předautorizace** - Transakce sloužící k předautorizaci zamýšlené platby a blokaci prostředků na účtu Držitele karty do doby dokončení předautorizace, nebo stanoveného časového limitu (např. pro dobu prověření podvodné transakce).
3. **Capture** - Platební transakce sloužící k dokončení příslušné předautorizace, zúčtování na vrub účtu Držitele karty a ve prospěch účtu obchodního partnera. Platba je ve stejné výši jako byla předautorizovaná částka. Transakce musí být provedena do sedmi kalendářních dnů od data autorizace (předautorizace).
4. **Partial capture/Částečná capture** - Platební transakce lišící se od capture pouze v tom, že částka ke zúčtování je nižší, než původní předautorizovaná. Používá se pokud obchodní partner není schopen dodat veškeré objednané zboží nebo služby, nebo pokud je dodávka realizována po etapách.
5. **Cancel/Zrušení** - Transakce sloužící ke zrušení předautorizace a tím k uvolnění blokace prostředků na účtu Držitele karty. Ruší vždy celou předautorizaci (nelze ji použít pokud již k předautorizaci byla zaslána capture nebo částečná capture). Používá se při odstoupení Zákazníka od objednávky, pokud ještě nebyla realizována a pokud to podmínky příslušného obchodního partnera připouštějí.

6. **Refund/Refundace** - Je platební transakce sloužící k vrácení zaplacené částky zpět z účtu obchodního partnera na účet Držitele karty. Vždy se vztahuje ke konkrétní dříve uskutečněné platbě, tj. nelze ji generovat jako nezávislou kreditní transakci a nemůže být vyšší, než původní platba. Použije se např. při uznané reklamaci a vrácení plné ceny zboží.
7. **Partial refund/Částečná refundace** - Je obdobou předešlé transakce s tím, že vrácená částka je menší, než byla původně zaplacená. Částečná refundace může být použita i opakovaně na stejné, nebo různé částky, dokud součet opakovaných dílčích částek refundace nedosáhne hodnoty původně zaplacené částky.
8. **Recurring/Opakovaný prodej** - Jedná se o periodicky opakované prodejní transakce s pevně stanovenou periodou a vždy stejnou částkou. První (inicializační) transakce je učiněna Držitelem karty, další transakce na základě parametrů zadaných Držitelem karty generuje automaticky POS Server.

2.3. Není podporován režim splátkového prodeje.

3. Potvrzení transakce

Potvrzení transakce je generováno ze strany obchodního partnera pro Držitele karty (zaslané e-mailem, faxem nebo dopisem) a zaslané během jednoho pracovního dne Zákazníkovi. Všechny nákupy v rámci jedné transakce musí být zahrnuty do jednoho Potvrzení transakce, které musí obsahovat:

- Název obchodního partnera odpovídající názvu na internetových stránkách obchodního partnera
- Aktuální adresu internetové stránky pro kontakt se Zákazníky
- Merchant ID – identifikace obchodního partnera v databázi ČS
- Kontakt na oddělení služeb zákazníkům – telefon a kód země. Pokud obchodní partner zasílá zboží/služby mezinárodně, musí uvést telefonní kontakt pro domácí i mezinárodní Držitele karet. Obchodní partner se zavazuje reagovat na reklamace a dotazy Zákazníků nejpozději do dvou pracovních dnů ode dne podání reklamace nebo dotazu.
- Částku a měnu transakce
- Datum transakce
- Identifikační číslo transakce (Merchant Refence Number)
- Typ transakce – debit, kredit, recurring
- Popis zboží/služeb včetně ceny (cena včetně nebo bez DPH)
- Identifikaci Zákazníka – jméno, adresa
- Podmínky a omezení prodeje
- V případě nabídky zboží na zkoušku (po určitou dobu zdarma) uvést přesné datum ukončení tohoto zkušebního období.
- Reklamační řád – odkaz na internetové stránky obchodního partnera
- Podmínky zrušení transakce
- Vybranou variantu, kterou Zákazník potvrdil v případě, že nebylo veškeré objednané zboží k dispozici.
- Doporučení pro Zákazníky, aby si vytiskli toto Potvrzení transakce pro případ reklamace.

4. Zaslání zboží

1. Obchodní partner si vyžádá údaje pro zaslání zboží:
   - Jméno Držitele karty
   - Název vydavatelské banky
   - Jméno a adresu příjemce - pro zaslání zboží (ne P.O.BOX)
   - Kontakt na příjemce – e-mail, telefon, fax
2. Obchodní partner doručí objednané zboží nebo službu pouze na určenou adresu příjemce (bydliště, pracoviště), uvedené v elektronické objednávce, a to do 30-ti dnů od proběhnutí transakce. Obchodní partner v žádném případě nedoručí objednané zboží na adresu poštovní schránky (P.O.BOX). Jako podezřelé je třeba posuzovat i opakované pokusy o změnu adresy doručení, nebo žádost o předání zboží na parkovišti, na recepci hotelu, řidiči taxislužby atd. V případě, že obchodní partner takovou podezřelou transakci přesto zrealizuje a tato bude následně držitelem karty neuznána a ČS bude v reklamačním řízení stranou neúspěšnou a vznikne jí škoda, obchodní partner takovou škodu ČS uhradí.

5. Potvrzení o převzetí zboží příjemcem nebo o poskytnutí služby příjemci

Obchodní partner zajistí písemné potvrzení o doručení zboží nebo služby příjemci, a to jak v případě osobního doručení obchodním partnerem, tak i v případě doručení třetí osobou (např. formou poštovní zásilky, prostřednictvím kurýrní služby, zásilkou prostřednictvím ČD). Za písemné potvrzení se považuje dokument, který obsahuje:

- Jméno a příjmení příjemce zboží nebo služby
- Číslo a druh průkazu totožnosti příjemce, podle kterého je obchodní partner nebo třetí osoba povinna při předávání zboží nebo poskytnutí služby ověřit totožnost.
- Datum převzetí zboží příjemcem nebo poskytnutí služby příjemci

6. Ohlašovací povinnost

1. Obchodní partner je povinen neprodleně hlásit jakýkoli únik nebo podezření na únik dat ze svého systému, případně podezření na využívání těchto dat třetí stranou.
2. Obchodní partner je povinen oznamovat ČS písemně v dostatečném předstihu, nejpozději však do 7 dnů před účinností takové skutečnosti, všechny změny, které mohou mít vliv na řádné plnění této Smlouvy, zejména:
   - změny bankovního spojení,

- změny adresy obchodního místa,
- změny doručovací adresy,
- změny sídla obchodního partnera,
- změny druhu či charakteru prodávaného zboží či poskytovaných služeb,
- změny v právním statutu obchodního partnera,
- jakékoli změny v obchodním rejstříku obchodního partnera,
- změny názvu obchodního partnera,
- zrušení obchodního místa,
- rozšíření obchodních míst obchodního partnera, která akceptují karty,
- změny názvu obchodního místa.

3. Obchodní partner je povinen ČS oznámit faxem, telefonicky, elektronickou poštou nebo písemně, nejpozději ve lhůtě 7 dnů před účinností této změny, následující změny:
   - změny faxového nebo telefonického spojení,
   - změny kontaktních osob.

---

7. Bezpečnostní standardy Asociací

Uvedené minimální požadavky bezpečnostních standardů stanovené Asociacemi jsou závazné jak pro obchodní partnery tak i pro všechny členské banky Asociací, včetně České spořitelny, a.s.

12 minimálních požadavků zabezpečení dat:

- Instalovat a aktualizovat (konfiguraci) firewall(u) pro ochranu dat držitelů platebních karet.
- Nepoužívat výchozí nastavení pro systémová hesla a jiné bezpečnostní parametry od dodavatele.
- Zabezpečit uložená data držitelů platebních karet.
- Šifrovat data držitelů platebních karet, přenášených přes veřejné sítě.
- Antivirový software je používán a pravidelně aktualizován.
- Vyvíjet a aktualizovat zabezpečení systémů a aplikací.
- Omezit přístup k datům držitelů platebních karet, týkajících se "utajovaných informací".
- Každé osobě s přístupem k počítači je přidělen jedinečný identifikační údaj.
- Omezit fyzický přístup k datům držitelů platebních karet.
- Kontrolovat a sledovat všechny přístupy k síťovým zdrojům a datům držitelů platebních karet.
- Pravidelně testovat zabezpečení systémů a procesů.
- Dodržovat zásady zabezpečení.

Další informace o bezpečnostních standardech Asociací jsou k dispozici na níže uvedených internetových stránkách :

http://www.visaeu.com/acceptingvisa/datasecurity.html
http://www.mastercardonline.com
https://www.pcisecuritystandards.org
https://www.pcistandards.cz

---

8. Součástí těchto Pokynů je příloha **Doporučené postupy pro transakce MO/TO a e-commerce.**